



**Cheshire College
South & West**



Data Protection Policy

Key Information	
Reference Number	CCSW - DPP
ELT Post Responsible for Update and Monitoring	Principal / CEO
Published on Website	No
Date approved by ELT	23 June 2026
Date Approved by Governor's Committee (if applicable)	08 July 2026
Date of Next Review	29 June 2029

I. Introduction

- I.1 The College needs to process information about its employees, suppliers (sole traders, partnerships or individuals within companies), students, governors, parents and visitors, contractors and volunteers.
- I.2 To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.
- I.3 The College and all staff or others who process or use any personal information must ensure that they always comply with Data Protection law and the Data Protection Principles (see section 4).
- I.4 To achieve this, the College shall:
 - I.4.1 ensure that personal data is processed lawfully, fairly and in a transparent manner in relation to individuals;
 - I.4.2 specify why the data is being collected and how it will be used (through a Privacy Statement);
 - I.4.3 ensure that personal information is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
 - I.4.4 only process personal information where the College has a specific legal basis to do so;
 - I.4.5 ensure that when dealing with the personal data of children the College complies with the law to ensure appropriate processing including appropriate processes for obtaining consent, where relevant, including compliance with the Age-Appropriate Design Code where relevant;
 - I.4.6 ensure that, where the College asks for consent to use personal data, people are asked to positively opt in, using clear, plain language that is easy to understand;
 - I.4.7 where consent is the lawful basis for processing personal data, tell individuals they can withdraw their consent at any time, the College shall ensure that individuals can refuse to consent without detriment and avoid making consent a precondition of a service;
 - I.4.8 ensure that all information is adequate, relevant and limited to what is necessary in relation to the purposes for which it is collected;
 - I.4.9 ensure that all information is kept accurate and, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified without delay;
 - I.4.10 implement appropriate record keeping standards and keep information in an identifiable form for no longer than is necessary for the purposes for which the personal data is obtained;
 - I.4.11 ensure information is protected against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and operational measures;
 - I.4.12 demonstrate accountability and compliance with these requirements through reports, appropriate documentation, training, spot checks and audits;
 - I.4.13 facilitate the rights of data subjects;
 - I.4.14 ensure that every instance where the College uses a data processor (a third party with access to process personal data) there is a written contract in place;
 - I.4.15 ensure that any transfers of personal data outside the UK comply with the law (*see section 6.8*);
 - I.4.16 conduct a Data Protection Impact Assessment (DPIA) (in line with the Data Protection Impact Assessment Policy and Procedure) where required to do so by law or best practice; and
 - I.4.17 report any data breaches promptly (in line with the Data Breach Management Procedure) and inform the Information Commissioners Office (ICO) and data subjects where required.

2. Status of the Policy

- 2.1 This Policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by the College from time to time. Any failures to follow the Policy can therefore result in disciplinary proceedings.
- 2.2 Any member of staff who considers that the Policy has not been followed in respect of personal data about them, should raise the matter with the Data Protection Officer initially. If the matter is not resolved, it should be raised as a formal grievance.
- 2.3 Compliance with data protection law is the responsibility of all members of the College. Any deliberate

breach of the Data Protection Policy may lead to disciplinary action being taken, or access to College facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the Data Protection Officer.

- 2.4 This policy will not discriminate either directly or indirectly against any individual on grounds of sex, race, ethnicity, sexual orientation, marital status, religion or belief, age, disability, or any other protected characteristics.

3. Roles and Responsibilities

- 3.1 Overall accountability for data protection sits with the Executive Leadership Team (ELT).

- 3.2 The ELT will:

- 3.2.1 champion a data protection culture in the organisation;
- 3.2.2 ensure that adequate resources are devoted to meet the College's data protection obligations;
- 3.2.3 commission reports from the Data Protection Officer and take action to remedy deficiencies identified by the report in a timely manner; and
- 3.2.4 ensure the Data Protection Officer operates independently and is not dismissed or penalised for performing their task (in relation only to their role as Data Protection Officer as defined in law).

- 3.3 Board of Governors

- 3.3.1 The Governors are responsible for holding the ELT to account to ensure compliance with the law.
- 3.3.2 The Data Protection Officer has a direct reporting line to the Governors where they can raise any data protection risks or compliance issues if necessary.

- 3.4 Operational responsibility for data protection sits with the College's Data Protection Officer

- 3.5 The Data Protection Officer will:

- 3.5.1 inform and advise all members of staff on their data protection obligations;
- 3.5.2 maintain the College's Data Protection registration, liaise with the Information Commissioner's Office and the College's legal advisers as required;
- 3.5.3 monitor compliance with data protection requirements;
- 3.5.4 contribute to the development and maintenance of all data protection policies, procedures and processes in relation to the protection of personal data;
- 3.5.5 advise and inform the College on any data protection impact assessment (DPIA), including monitoring performance of DPIAs;
- 3.5.6 report and advise ELT on the allocation of their responsibilities to support ongoing compliance Data Protection law;
- 3.5.7 provide data protection training and awareness to all members of staff;
- 3.5.8 conduct audits of processes relating to personal data;
- 3.5.9 be the point of contact for data subjects about the processing of their personal data and respond to all data subject access request;
- 3.5.10 co-ordinate and advise on all non-routine requests for disclosure of personal information;
- 3.5.11 advise senior management on the allocation of information security responsibilities;
- 3.5.12 develop/advise on formal procedures for reporting incidents and investigations;
- 3.5.13 contribute to the risk management, business continuity and disaster recovery planning process;
- 3.5.14 advise on and monitor organisational record management and retention arrangements;
- 3.5.15 ensure that records of the processing are kept and the College Notifies the ICO;
- 3.5.16 advise on the issuing of privacy notices to data subjects at the point of collection of their personal data;
- 3.5.17 be the first point of contact for any enquiries from the Information Commissioners Office (and any EU supervisory authorities, where relevant); and

3.5.18 deal with any data breaches/complaints.

3.6 All staff also have responsibility for data protection. All staff must:

- 3.6.1 ensure any personal data which they hold is kept securely;
- 3.6.2 check that any information that they provide to the College in connection with their employment is accurate and up to date;
- 3.6.3 ensure personal information is not disclosed either orally or in writing, accidentally or otherwise unlawfully to any unauthorised party;
- 3.6.4 only access personal data that is applicable and required for them to undertake their role;
- 3.6.5 report a data breach immediately when any data breach occurs;
- 3.6.6 undertake all required data protection/cyber security training;
- 3.6.7 always maintain data protection awareness reporting any data protection risks or concerns to their Line Manager or the Data Protection Officer;
- 3.6.8 Not to remove personal data, or devices containing, or that can be used to access personal data, from the College without applying the appropriate security measures (such as encryption) to secure the data and the device;
- 3.6.9 Not to store personal data on local drives, or on personal devices that are used for work purposes.
- 3.6.10 ensure that records are accurate, kept up to date kept securely and disposed of safely in accordance with the timescales set out in this and other relevant record keeping procedures;
- 3.6.11 To keep data secure (for example by complying with rules on access to premises, password protection);
- 3.6.12 only send marketing information if they have approval from the Marketing Department and Data Protection Officer;
- 3.6.13 not process Special Categories of data or Criminal offence data without first ensuring they have a legal basis to do so and recording this processing with the Data Protection Officer;
- 3.6.14 ensure they have an appropriate contract in place (approved by the Data Protection Officer) with any third-party organisation that will have access to personal data (*see section 6.8*);
- 3.6.15 where staff are required to sending personal data to another country (*see section 6.8*); or international organisations, they must seek advice from the Data Protection Officer ;
- 3.6.16 check that any information that they provide to the College in connection with their employment is accurate and up to date and inform the College of any changes to information which they have provided, e.g., change of address or name; and
- 3.6.17 follow all guidance relating to information sharing.

3.7 Students are responsible for:

- 3.7.1 checking that the information they provide to the College in connection with their enrolment is accurate and up to date;
- 3.7.2 informing the College of any changes to the information they provide, such as, change of address, emergency contact details;
- 3.7.3 not seeking to gain unauthorised access to personal information; and
- 3.7.4 complying with all College policies regarding the use of IT facilities.

3.8 Managers are responsible for ensuring they:

- 3.8.1 are satisfied with the legality of holding and using the information collected by staff in their area; and
- 3.8.2 keep the College data documentation controller spreadsheet up to date based on their areas of responsibility;
- 3.8.3 ensuring that the use of personal data complies with all appropriate college policies;
- 3.8.4 ensuring that relevant staff they manage, undertake the Data Protection training;
- 3.8.5 referring any non-routine requests for disclosure, requests for subject access and requests to cease processing to the Data Protection Officer;
- 3.8.6 raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay; and
- 3.8.7 checking and approving with third parties that handle the company's data any contracts or agreement

regarding data processing;

3.9 The Network Services/IT Systems Team are responsible for:

- 3.9.1 Whilst all staff and users of personal data have some responsibility for the security of data, Computer Services and Information Systems staff have an important role in ensuring the security of computerised data. In particular, they will:
 - 3.9.1.1. be responsible for advising the College on the state of technological development with regard to IT security;
 - 3.9.1.2. provide secure methods of transferring authorised personal data outside the College;
 - 3.9.1.3. back up data on the College's IT systems and have disaster recovery procedures in place and tested;
 - 3.9.1.4. implement virus detection and hacking preventative measures;
 - 3.9.1.5. through liaison with the appropriate manager, ensure that the College's business systems are secure and appropriate restrictions on access are in place so that individuals only have access to personal data in which they have a legitimate business interest;
 - 3.9.1.6. require the use of passwords and ensure they are changed regularly;
 - 3.9.1.7. produce and update policies for the use of College IT facilities including email, intranet, and internet;
 - 3.9.1.8. investigate breaches of IT security; and
 - 3.9.1.9. Ensure that data is deleted according to the College's Retention of Personal Data Policy.

3.10 The Marketing Team are responsible for:

- 3.10.1 approving data protection statements attached to emails and other marketing copy; and
- 3.10.2 addressing data protection queries from clients, target audiences or media outlets.

3.11 The Human Resources Team will:

- 3.11.1 ensure that the College's Employment Practices are consistent with the Employment Codes of Practice;
- 3.11.2 ensure that Data Protection obligations are reflected in the College's Disciplinary Procedures and contracts of employment;
- 3.11.3 ensure that all staff are aware of the types of personal information that the College will process on them and ask staff to check this information as required;
- 3.11.4 ensure that all obligations outlined within the Disclosure and Barring Service (DBS) Code of Practice published under section 122 of the Police Act 1997 are adhered to. Full details of the CRB Code of Practice can be found at [this link](#).
- 3.11.5 provide advice to managers and others on the application of the DBS Code of Practice; **and**
- 3.11.6 destroy personal data according to the College's Retention of Personal Data Policy.

4 Data Protection Principles

4.1 When using Personal Data, Data Protection Laws require that the College complies with the following principles. These principles require Personal Data to be:

- 4.1.1 Processed lawfully, fairly and in a transparent manner;
- 4.1.2 Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- 4.1.3 Adequate, relevant, and limited to what is necessary for the purposes for which it is being processed;
- 4.1.4 Accurate and kept up to date, meaning that every reasonable step must be taken to ensure that Personal Data that is inaccurate is erased or rectified as soon as possible;
- 4.1.5 Kept for no longer than is necessary for the purposes for which it is being processed;
- 4.1.6 Processed in a manner that ensures appropriate security and integrity of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or

damage, using appropriate technical or organisational measures.

5 Lawful Use of Personal Data

- 5.1 In order to collect and/or use personal data lawfully the College needs to be able to show that its use meets one of a number of legal grounds. Please click here to see the detailed grounds [<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing>].
- 5.2 In addition, when the College collects and/or uses special categories of personal data, the College has to show that one of a number of additional conditions is met. Please click here to see the detailed additional conditions [<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/special-category-data>].
- 5.3 The College has carefully assessed how it uses personal data and how it complies with the obligations set out in *paragraphs 5.1 and 5.2*. If the College changes how it uses personal data, the College needs to update this record and may also need to notify Individuals about the change. If college personnel therefore intend to change how they use personal data at any point they must notify the Data Protection Officer who will decide whether their intended use requires amendments to be made and any other controls which need to apply.
- 5.4 Where Special Category Personal Data or Criminal Offence Data is processed, the College will ensure that an additional condition under UK GDPR and the Data Protection Act 2018 is identified and documented.
- 5.5 Staff proposing new processing activities must consult the Data Protection Officer to ensure the lawful basis has been identified and recorded.

6 Disclosing/Sharing Personal Data

- 6.1 Data Sharing General Principles:
 - 6.1.1 personal data must generally not be disclosed either orally or in writing, accidentally or otherwise to any unauthorised third party; and
 - 6.1.2 the College must ensure that individuals are informed if their data is to be shared with another organisation. Where sharing is to take place on a regular basis a data sharing agreement may be required. Data sharing agreements can be obtained from the Data Protection Officer.
- 6.2 Parents/Guardians/Carers:
 - 6.2.1 learners are advised that it is College policy that staff may contact named parents/guardians of learners under the age of 18 at the start of the course to discuss academic progress, attendance and conduct. Learners who do not wish the College to make such contact may be granted an exemption by writing to the Principal at the commencement of their course;
 - 6.2.2 learner Administration will provide a list of such learners which will be circulated to appropriate curriculum leaders.. If the learner has requested that the College does NOT contact their parents/guardians, then no information can be given;
 - 6.2.3 the learner will have indicated on the enrolment form the name of the parent/guardian with whom contact can be made. Learners can change these details on the system; and
 - 6.2.4 enquiries can be dealt with, generally by the Personal Development Tutor (PDT) or Assistant Director (AD) or Centre Principals, but only with the person given by the learner using the contact details on the learner record.
- 6.3 Other Family Members, Friends etc:
 - 6.3.1 staff should not respond to any enquiries from other family members or friends and should not even confirm that someone is a learner at the College. If the reason for the enquiry is stated to be an emergency, then the matter should be referred to the duty manager/member of the Senior leadership Team (SLT).
- 6.4 Potential Employers and Education Institutions (Reference Requests):

6.4.1 these should be dealt with by the Personal Development Tutor (PDT) and/or curriculum teams. All reference requests and responses should be in writing. The learner is entitled to see copies of any reference written about them. Copies of all references should be kept in the learner file.

6.5 Government Agencies:

6.5.1 government agencies can include, but not be limited to, Social Services, Police, Benefits agencies, probation service, tax etc;

6.5.2 the College is legally bound to provide information to various government agencies. All requests for information and all responses should be in writing. Copies of all requests should be kept centrally by the Data Protection Officer and

6.5.3 staff should seek advice from the Data Protection Officer when responding to any such requests.

6.6 Data Controllers:

6.6.1 a data controller is a third party which the College shares to process personal data and the third-party chooses how to use this data; and

6.6.2 a list of Data Controllers will be maintained by the Legal Advisor / Data Protection Officer.

For Example:

Where a learner is undertaking a work experience placement details about the learner are provided to the employer. The employer is themselves a Data Controller and is responsible for how it handles this information and must do so in line with data protection law.

6.7 Data Processors:

6.7.1 A data processor is a third party which the College uses to process personal data. In every case where the College uses a data processor it will ensure it has a written contract in place. The contract is important so that both parties understand their responsibilities and liabilities. A list of contracts will be maintained by the Legal Advisor/Data Protection Officer.

6.7.2 The contract must include the following:

- subject matter and duration of the processing;
- nature and purpose of the processing;
- type of personal data and categories of data subject; and
- obligations and rights of the controller.

6.7.3 the contract will require that the processor must:

- only act on the written instructions of the organisation (unless required by law to act without such instructions).
- ensure that people processing the data are subject to a duty of confidence.
- take appropriate measures to ensure the security of processing.
- only engage a sub-processor with the prior consent of the data Society and a written contract.
- assist the organisation in providing subject access and allowing data subjects to exercise their rights.
- assist the organisation in meeting its obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments.
- delete or return all personal data to the organisation as requested at the end of the contract.
- submit to audits and inspections, provide the organisation with whatever information it needs to ensure that they are both meeting their data protection obligations and tell the organisation immediately if it is asked to do something infringing the law.

6.8 Transferring personal data to a country outside the EEA

6.8.1 Data Protection Laws impose strict controls on Personal Data being transferred outside the EEA. Transfer includes sending Personal Data outside the EEA but also includes storage of Personal Data or access to it outside the EEA.

6.8.2 It needs to be thought about whenever the College appoints a supplier outside the EEA or the College appoints a supplier with group companies outside the EEA which may give access to the Personal Data to staff outside the EEA. So that the College can ensure it is compliant with Data Protection Laws

College Personnel must not export Personal Data unless it has been approved by the Data Protection Officer and Executive Leadership Team.

- 6.8.3 College Personnel must not export any Personal Data outside the EEA without the approval of the Data Protection Officer and the Executive Leadership Team.

7 Transparent Processing - Privacy Policy

- 7.1 Where the College collects personal data directly from individuals it will comply with the rights of the data subject including the right to inform them about how the College uses their personal data. This is in a privacy policy.
- 7.2 If the College receives personal data about an Individual from other sources, the College will provide the individual with a privacy policy about how the College will use their personal data. This will be provided as soon as reasonably possible and in any event within one month.
- 7.3 If the College changes how it uses personal data, the College may need to notify individuals about the change. If college personnel therefore intend to change how they use personal data, please notify the Data Protection Officer who will decide whether the College Personnel's intended use requires amendments to be made to the privacy notices and any other controls which need to apply.

8 Retention of Personal Data

- 8.1 Data Protection Laws require that the College does not keep Personal Data longer than is necessary for the purpose, or purposes for which the College collected it.
- 8.2 The College has assessed the types of Personal Data that it holds and the purposes it uses it for and has set retention periods for the different types of Personal Data processed by the College, the reasons for those retention periods and how the College securely deletes Personal Data at the end of those periods. These are set out in the Data Retention Policy.
- 8.3 All Staff have a responsibility to comply with the College Data Retention Policy and the retention period defined within it ensuring that personal data that has reached the end of its retention period is either destroyed, or anonymised. (Data which has been anonymised so that identifying information has been removed from its content, may be kept by the College for an indefinite period).
- 8.4 If College Personnel feel that a particular item of Personal Data needs to be kept for more or less time than the retention period set out in the Data Retention Policy, for example because there is a requirement of law, or if College Personnel have any questions about this Policy or the College's Personal Data retention practices, they should contact the Data Protection Officer for guidance.
- 8.5 In circumstances where an individual submits a request for their personal data to be deleted, the College will take account of its Data Retention Policy to see if there are reasons why it may not be appropriate to comply with the request i.e. when it is necessary to retain the data due to a legal, statutory, regulatory, or security reason.

9 Record Disposal

- 9.1 The College has robust processes in place to ensure that personal data is disposed in a way that protects the rights and privacy of data subjects (e.g. disposal via confidential waste, shredding), destruction of personal data must include all copies/backups. Personal Data which will not be destroyed will be that pending an investigation, litigation, or audit, or being processed as part of an outstanding subject access request.

10 Data Security

- 10.1 The College takes information security very seriously and the College has security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data. The College has in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction.

- 10.2 All College Personnel are responsible for ensuring the personal data they process is managed and kept secure aligned with College Policy and not shared with any unauthorised party.
- 10.3 Personal Data must only be accessed by individuals who as a part of their responsibilities/association with the College need to use it. On all occasions electronic data should be stored securely, password protected in alignment with College Procedures. Alternatively, hard paper copy must be stored in locked cabinets.
- 10.4 Processing of personal data off college premises should be undertaken in accordance with the policy and procedures.

11 Data Breach

- 11.1 Whilst the College takes information security very seriously, unfortunately, in today's environment, it is possible that a security breach could happen which may result in the unauthorised loss of, access to, deletion of or alteration of Personal Data. If this happens there will be a Personal Data breach and College Personnel must comply with the College's Data Breach Notification Policy.
- 11.2 Personal Data breach is defined very broadly and is effectively any failure to keep Personal Data secure, which leads to the accidental or unlawful loss (including loss of access to), destruction, alteration, or unauthorised disclosure of Personal Data. Whilst most Personal Data breaches happen as a result of action taken by a third party, they can also occur as a result of something someone internal does.
- 11.3 If the College discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The College will record all data breaches regardless of their effect.
- 11.4 Any data breaches must be reported using the form at Appendix I and sent to the College Data Protection Officer.
- 11.5 There are three main types of Personal Data breach which are as follows:
 - 11.5.1 **Confidentiality breach** - where there is an unauthorised or accidental disclosure of, or access to, Personal Data e.g. hacking, accessing internal systems that a College Personnel is not authorised to access, accessing Personal Data stored on a lost laptop, phone or other device, people "blagging" access to Personal Data they have no right to access, putting the wrong letter in the wrong envelope, sending an email to the wrong student, or disclosing information over the phone to the wrong person;
 - 11.5.2 **Availability breach** - where there is an accidental or unauthorised loss of access to, or destruction of, Personal Data e.g. loss of a memory stick, laptop or device, denial of service attack, infection of systems by ransomware, deleting Personal Data in error, loss of access to Personal Data stored on systems, inability to restore access to Personal Data from back up, or loss of an encryption key; and
 - 11.5.3 **Integrity breach** - where there is an unauthorised or accidental alteration of Personal Data.
- 11.6 In circumstances, where an individual either suspects or discovers a personal data breach including unauthorised, or unlawful processing, accidental loss, destruction, or damage to personal data they have a responsibility to report it immediately in accordance with the College Data Breach Policy. The Data Protection Officer must also immediately be notified to enable the appropriate action to be initiated.
- 11.7 Where a data breach has occurred as a result of misconduct, or malicious intent it is considered to be an offence and, in such circumstances the College's Disciplinary Policy would be initiated and action being taken, access to college facilities being withdrawn, or even a criminal conviction.

12 Appointing Contractors Who Access the College's Personal Data

- 12.1 If the College appoints a contractor who is a Processor of the College's Personal Data, Data Protection Laws require that the College only appoints them where the College has carried out sufficient due diligence and only where the College has appropriate contracts in place.
- 12.2 One requirement of the Data Protection Act is that a Controller must only use Processors who meet the

requirements of the Act and protect the rights of individuals. This means that data protection due diligence should be undertaken on both new and existing suppliers. Once a Processor is appointed, they should be audited periodically to ensure that they are meeting the requirements of their contract in relation to Data Protection.

- 12.3 Any contract where an organisation appoints a Processor must be in writing.
- 12.4 You are considered as having appointed a Processor where you engage someone to perform a service for you and as part of it, they may get access to your Personal Data. Where you appoint a Processor you, as Controller remain responsible for what happens to the Personal Data.
- 12.5 The Data Protection Act requires the contract with a Processor to contain the following obligations as a minimum:
- To only act on the written instructions of the Controller;
 - To not export Personal Data without the Controller's instruction;
 - To ensure staff are subject to confidentiality obligations;
 - To take appropriate security measures;
 - To only engage sub-processors with the prior consent (specific or general) of the Controller and under a written contract;
 - To keep the Personal Data secure and assist the Controller to do so;
 - To assist with the notification of Data Breaches and Data Protection Impact Assessments;
 - To assist with subject access/individuals' rights;
 - To delete/return all Personal Data as requested at the end of the contract;
 - To submit to audits and provide information about the processing; and
 - To tell the Controller if any instruction is in breach of the Data Protection Act, or other EU state data protection law.
- 12.6 In addition, the contract should set out:
- The subject-matter and duration of the processing;
 - The nature and purpose of the processing;
 - The type of Personal Data and categories of individuals; and
 - The obligations and rights of the Controller.

13 Individuals' Rights

- 13.1 The College will use all Personal Data in accordance with the rights given to Individuals under Data Protection Laws and will ensure that it allows Individuals to exercise their rights in accordance with the College's Rights of Individuals Policy and Rights of Individuals Procedure. Please familiarise yourself with these documents as they contain important obligations which College Personnel need to comply with in relation to the rights of Individuals over their Personal Data. Full details of this are covered in the College's Data Rights procedure.

14 Marketing and Consent

- 14.1 The College will sometimes contact individuals to send them marketing or to promote the College. Where the College carries out any marketing, Data Protection Laws require that this is only done in a legally compliant manner. The College will identify and document the appropriate lawful basis for direct marketing activity. In many cases this will be consent. Where permitted by law, including where PECR does not require consent, the College may rely on legitimate interests where it has carried out and documented an appropriate assessment and has concluded that the marketing is proportionate, would not be unexpected, and does not override the rights and freedoms of the individual. Where consent is relied upon, records of consent will be retained for as long as needed to demonstrate compliance.
- 14.2 The College will provide in each direct marketing communication a clear and easy way for individuals to opt out or unsubscribe. Where an individual objects to direct marketing, or withdraws consent where consent is the lawful basis, the College will stop sending direct marketing to that individual and will action the request within 30 days.

- 14.3 Where the College relies on consent for direct marketing, it may from time to time contact individuals to give them the opportunity to update their details and confirm that they wish to continue receiving promotional material. Where the College relies on legitimate interests, it will keep the appropriateness of that lawful basis under review and ensure individuals are reminded of their right to object.

15 CCTV

- 15.1 The College Close Circuit Television complies with the laws relating to data protection, and includes the principles governing the processing of personal data

16 Automated Decision Making and Profiling

- 16.1 Under Data Protection Laws there are controls around profiling and automated decision making in relation to Individuals.

16.1.1 Automated Decision Making happens where the College decides about an Individual solely by automated means without any human involvement and the decision has legal or other significant effects.

16.1.2 Profiling happens where the College automatically uses Personal Data to evaluate certain things about an Individual.

- 16.2 Any Automated Decision Making or Profiling which the College carries out can only be done once the College is confident that it is complying with Data Protection Laws. If College Personnel therefore wish to carry out any Automated Decision Making or Profiling College Personnel must inform the Data Protection Officer.

- 16.3 College personnel must not carry out Automated Decision Making or Profiling without the approval of the Data Protection Officer.

- 16.4 The College allows for individuals to request human intervention into any significant automated decision making.

17 Data Protection Impact Assessments (DPIA)

- 17.1 A DPIA should be started as early as practical in the design of processing operations. A DPIA is not a prohibition on using Personal Data but is an assessment of issues affecting Personal Data which need to be considered before a new product/service/process is rolled out. Full details of the College's approach to DPIAs' is covered in our Data Protection Impact Assessment Procedure.

- 17.2 All DPIAs must be reviewed and approved by the Data Protection Officer.

18 Review and Monitoring

- 18.1 The relevance, efficiency and effectiveness of this Data Protection Policy will be reviewed in line with the annual cycle of strategic management activities to facilitate continuous improvement. The results of the review process will be analysed and changes made to the policy where appropriate.

Appendix I - Key Definitions

Term	Definition
College	Cheshire College South and West including Crewe, Ellesmere Port, Chester and Macclesfield campus
College Personnel	Any College employee, worker or contractor who accesses any of the College's Personal Data and will include employees, consultants, contractors, and temporary personnel hired to work on behalf of the College.
Personal Data	'Personal data' means any information relating to an identifiable person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Special Categories of Personal Data	'Special categories of personal data' are racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a person's sex life or sexual orientation. Note: This was previously referred to as Sensitive Personal data.
Data Protection Principals	Data Protection law sets out seven key principles: • lawfulness, fairness and transparency; • purpose limitation; • data minimisation; • accuracy; • storage limitation; • integrity and confidentiality (<i>security</i>); and • accountability.
Processing	'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Data Controller	'Controller' any person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. A Controller is responsible for compliance with Data Protection Laws. Examples of Personal Data the College is the Controller of include employee details or information the College collects relating to students. The College will be viewed as a Controller of Personal Data if it decides what Personal Data the College is going to collect and how it will use it.
Data Processor	'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. A Processor is a third party that processes Personal Data on behalf of a Controller. This is usually as a result of the outsourcing of a service by the Controller or the provision of services by the Processor which involve access to or use of Personal Data. Examples include where software support for a system, which contains Personal Data, is provided by someone outside the business; cloud arrangements and mail fulfilment services.
UK Data Protection Law	Refers to the applicable laws of the land including the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Privacy and Electronic Communications Regulations (PECR), the Data (Use and Access) Act 2025, and any subsequent legislation, statutory instruments, codes of practice or guidance issued by the Information Commissioner's Office (ICO).
Data Protection Officer	Our Data Protection Officer is
DPIA	A Data Protection Impact Assessment is a document that needs to be completed wherever the processing of personal data represents a high level of risk to the individual's rights and freedoms.
EEA	Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany , Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden.
ICO	The Information Commissioner's Office, the UK's data protection regulator.
Special Categories of Personal Data	Personal Data that reveals a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data (i.e. information about their inherited or acquired genetic characteristics), biometric data (i.e. information about their physical, physiological or behavioural characteristics such as facial images and fingerprints), physical or mental health, sexual life or sexual orientation and criminal record. Special Categories of Personal Data are subject to additional controls in comparison to ordinary Personal Data.

Appendix 2 – Data Protection Requirements

1. Physical Security:
 - staff must always wear their ID badge;
 - staff must never allow others to use their swipe cards or pin numbers to gain entry;
 - staff must not allow others to 'tailgate' e.g., follow a staff member through secure areas;
 - staff must report to security personnel if they encounter unescorted visitors or anyone not wearing appropriate visible identification, (i.e., an ID badge); and
 - boards displaying person identifiable data should be sited in areas not accessible to learners or the public.
2. Paper Records:
 - all paper and files containing data subject details to be securely locked away when not in use a clear desk policy should be adopted; and
 - data that is no longer required must be disposed of securely. The College uses a secure shredding company to dispose of data securely.
3. Working Remotely/Offsite:
 - physical records must only be taken off-site where absolutely necessary;
 - only take the minimum necessary personal information off site;
 - ensure that staff members have a secure place to protect manual information;
 - never leave personal information in an unsecure area in the home, i.e., in garages, sheds, boots of cars, near open doors or windows;
 - never work on personal information in a public place where it could be seen by a third party; and
 - prevent access to information by other members of the household and by visitors. Staff members working at home should ensure they adopt a clear desk policy when leaving their work unattended.
4. Transporting Paper Records:
 - keep information in a sealed container/bag;
 - public transport should not be used for transporting personal information, if an exception to this rule is identified the information must be transported in a locked briefcase or similar;
 - never leave information unattended in the car for an extended length of time; and
 - never leave information in the boot of a car overnight. Information must be taken inside a property and secured.
5. Moving Offices/Relocation of Working Area:
 - all records should be either: transferred to a secure area for continued storage in the new location, archived or destroyed in line with the College Retention Schedule;
 - all filing/storage cabinets should be transferred to the new office, or those remaining for removal or disposal must be checked to ensure they are empty of all paperwork and IT devices;
 - all desk draws should be opened and the desks inspected to ensure they are empty of all paperwork and IT devices;
 - all rooms including cupboards, kitchens and other storage spaces must be checked to ensure they are empty of all paperwork or IT devices;
 - all confidential waste must be shredded or placed in clearly marked confidential waste collection bins/bags and a collect must be arranged; and
 - all IT equipment including laptops, desktops, DVDs, floppy disks, memory sticks etc. has been transferred to the new work area or returned to IT for secure disposal.
6. Post:
 - all external post should be delivered to the Post Room which must be locked when not staffed;
 - sensitive information should be posted using tracked services;
 - post should not be left in unsupervised areas that are open to learners or the general public; and
 - post containing personal or confidential information should be sent in sealed envelopes.
7. IT Security:
 - screens of computers must always be locked when left unattended;
 - if electronic data is stored on removable media, these must be encrypted and kept locked away securely when not in use; and

- electronic data should only be stored on the College's designated drives and servers and should only be uploaded to an approved cloud computing services that the College has a contract with (e.g., do not use Dropbox, Google Drive etc.).

8. Email:

- staff should always consider if email is the best communication method;
- staff should always consider whether the e-mail going to just one person. If so, is it the correct person where similar names exist in the e-mail directory or address book;
- staff should always consider whether to use the 'reply all' function. If so, does every person on the list need to receive the reply and any attachment;
- staff should carefully check the recipients of all e-mails prior to sending regardless of content. Staff members should be extra vigilant where personal, sensitive personal or confidential information is included;
- always delete emails which they have reached their retention period;
- only send email from another member of staff's email account or under an assumed name if they have the specific authority. This is generally reserved for the Executive Leadership Team.
- manage email appropriately, clearing the deleted items folder and using appropriate archiving facilities; and
- use password protect the content of any email when sending sensitive/confidential/special categories of data.

9. Telephone:

- staff should generally not give any information about a learner, not even confirmation that an individual is a learner at the College, in response to any telephone enquiry, even if the query is from the parents unless they have taken steps to verify the caller such as asking for specific information, such as learner date of birth, course attending etc; and
- wherever possible it is recommended that staff:
- take the name and telephone number of the person calling;
- ask the nature of the enquiry;
- tell the caller that you will pass on the enquiry or telephone them back;
- seek advice from their line manager or the Data Protection Officer; and
- enquiries about a learner's progress or attendance should be passed on to the Personal Development Tutor (PDT) Attendance Co-ordinator.

10. Marketing:

- there are specific rules around sending advertising or marketing material which is directed to specific individuals. Routine service messages do not count as direct marketing, such as correspondence to provide information they need about the College (e.g., information about College closures due to bad weather, safety announcements, changes to term dates etc.). General branding, logos or straplines in these messages do not count as marketing;
- when sending specific marketing messages, staff should have obtained consent to send any emails, texts, picture messages, video messages, voicemails, direct messages via social media or any similar electronic messages; and
- all uses personal data to directly target individuals for marketing purposes should be reviewed with the Data Protection Officer.

11. Retention:

- the College must ensure that personal data is kept no longer than is necessary;
- records which have reached the end of their life (whether held in electronic or paper format) should generally be destroyed under confidential conditions. Once a document reaches its retention period it should be reviewed to ensure it does not need to be kept for longer as some records need to be kept for historical purposes and these will be transferred to a place of deposit by the Data Protection Officer. Any staff wishing to retain a record for longer than the specified retention period should contact the Data Protection Officer for advice and guidance;
- a Document Retention Procedure has been produced and staff must review this policy and ensure records are kept in line with the timescales specified. Staff must ensure that once data has reached its retention period it is destroyed securely. All personal data held in paper form must be disposed of by shredding or in the shred bins provided on College premises; and
- electronic media will be disposed of securely by the Network Services.